



National Transportation Safety Board

Washington, D.C. 20594

Office of the Chairman

AUG 08 2006

Mr. Todd Zinser
Acting Inspector General
Department of Transportation
400 7th Street S.W., Room 9210
Washington, D.C. 20590

Dear Mr. Zinser:

I am in receipt of a letter dated August 4, 2006, from Rebecca Leng, Assistant Inspector General for Financial and Information Technology Audits. Her letter announces your intent to begin a limited review of the National Transportation Safety Board's (NTSB) information security program in support of reporting requirements under the Federal Information Security Management Act of 2002 (FISMA). My staff looks forward to working with you as you conduct this review.

We appreciate Ms. Leng's recognition of the NTSB's information security efforts. Ms. Leng's letter specifically mentions NTSB having established a Chief Information Officer (CIO) position, submitting progress reports to Congress, and to your office, providing security training to all employees, and enhancing network security. I would point out that the NTSB not only established the position of CIO, but we also named a Chief Information Security Officer (CISO) and we realigned all information technology staff into a newly-created office that now reports directly to the Managing Director. Further, the security training that Ms. Leng noted was provided not just to employees, but to *everyone* who has access to the NTSB computer network. Further, several of our key information technology staffers have attended a variety of courses on advanced FISMA and information security topics. Other major accomplishments include the implementation of an agency-wide screen saver lockout, the addition of security warning banners to network logon screens, and the roll out of several new Operations Bulletins (policy documents) pertaining to information security. Finally, the NTSB made a timely submission of its Program of Actions and Milestones to the Office of Management and Budget.

I was concerned and somewhat disappointed to read Ms. Leng's statement that the NTSB did not make sufficient progress "...reviewing, testing, certifying, and accrediting its information systems as adequately secured to support NTSB operations." The activities described in the paragraph above represent a significant commitment to information security and to FISMA compliance, and they will provide a solid framework for certifying and accrediting the NTSB's information systems. More importantly, in October 2005, following your 2005 evaluation of our information security program, NTSB Managing Director Joseph Osterman developed a milestone plan of action to bring the agency into FISMA compliance. At that time, Rebecca

Leng noted that our plan was "...a very good road map to get NTSB's information security program back on the right track."

The NTSB has met each of the deadlines agreed to in our milestone plan, and my staff has met with yours on several occasions to ensure that you are aware of our accomplishments and efforts. I am concerned that the evaluation criteria seem to have now been changed and we are being criticized for doing exactly what we agreed to and set out to do.

Ms. Leng's letter asks us to consider two suggestions: disaggregating our system inventory, and conducting more risk assessments. Although the NTSB will consider these suggestions, we believe that because our staff is most familiar with our information systems and business practices, our agency is in the best position to inventory and assess the risk of our systems. I note that FISMA, as codified at Title 44 United States Code § 3544, gives the responsibility for conducting system inventories and risk assessments to each agency head, and I take this responsibility very seriously.

We look forward to working with you as you conduct your review of our information security program.

Sincerely,

A handwritten signature in black ink, appearing to read "Mark V. Rosenker", written in a cursive style.

Mark V. Rosenker
Acting Chairman